(分散ストレージシステムにおける) Rashmi-Shah-Kumar 再生成符号の拡張と秘密分散について

On an extended version of Rashmi-Shah-Kumar regenerating codes and secret sharing for distributed storage

栗原 正純　　　桑門 秀典
(電気通信大学)　(神戸大学)

電子情報通信学会 情報理論研究会 (サブソ合同研究会) 大阪大学吹田キャンパス

2011/03/03-04

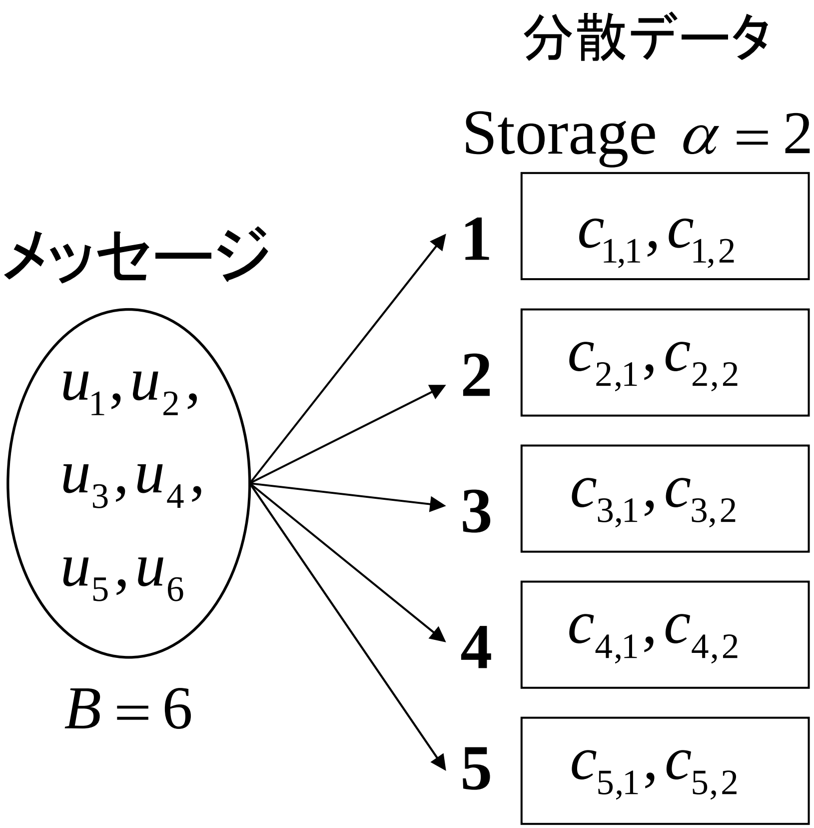
Masazumi Kurihara (kuri@ice.uec.ac.jp)

分散ストレージシステムの修復問題と再生成符号 I

1. **分散ストレージシステムの修復問題**
   [1] A.G.Dimakis, P.B.Godfrey, Y.Wu, M.J.Wainwright
   and K.Ramchandran,
   ”Network Coding for Distributed Storage Systems,”2010.
2. **再生成符号** (Regenerating codes)
   1. **復元**:
      → **オリジナルデータの復元**
   2. **修復** (**再生成**):
      → **故障ノードの修復（システムの信頼性の維持）**
      → **故障ノードに保存されていたデータの再生成**

分散ストレージシステム（信頼性）

$(k=3)$



$\boxed{u_k, c_{j,k} \in GF(q)}$

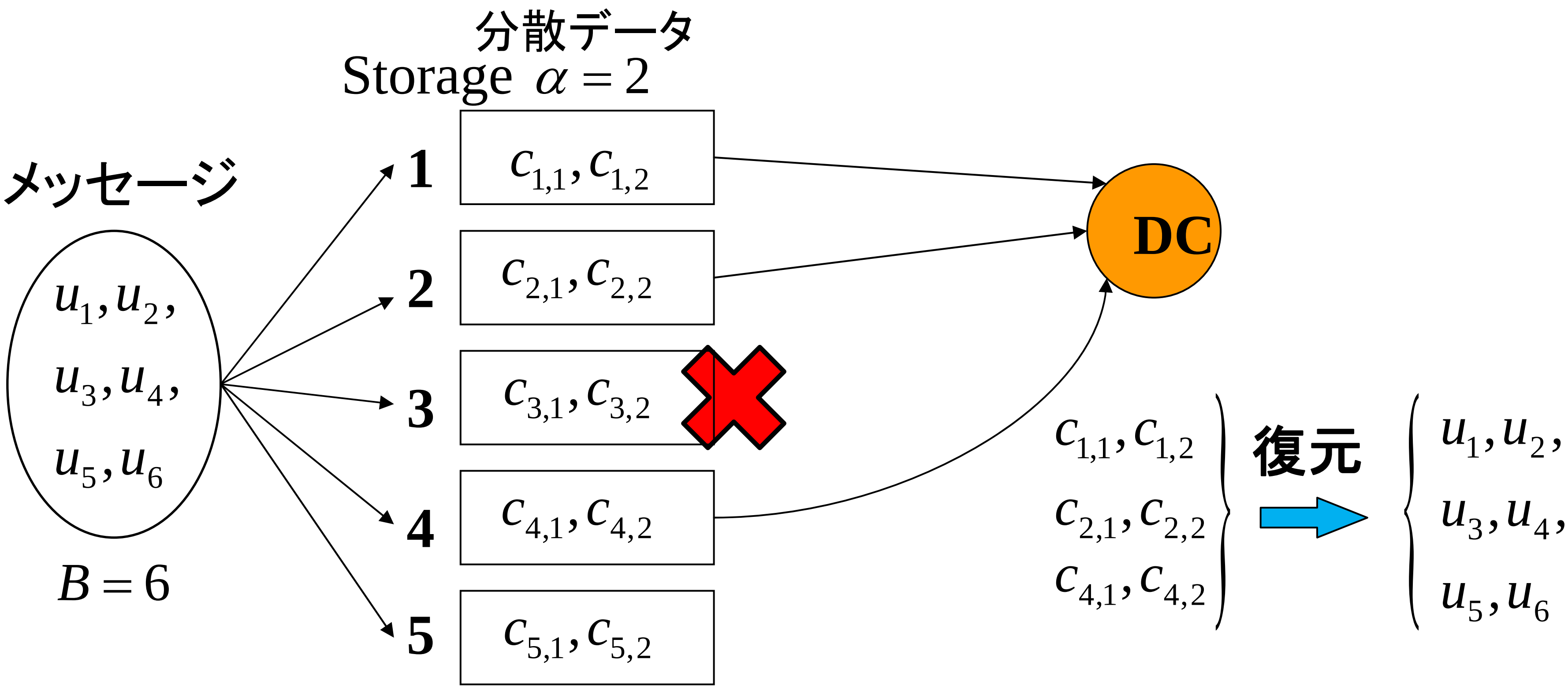
分散符号化

ノード i

メッセージ $\left.\begin{matrix} u_1, u_2, \\ u_3, u_4, \\ u_5, u_6 \end{matrix}\right\} \Rightarrow \left\{ c_{i,1}, c_{i,2} \right.$ 分散データ

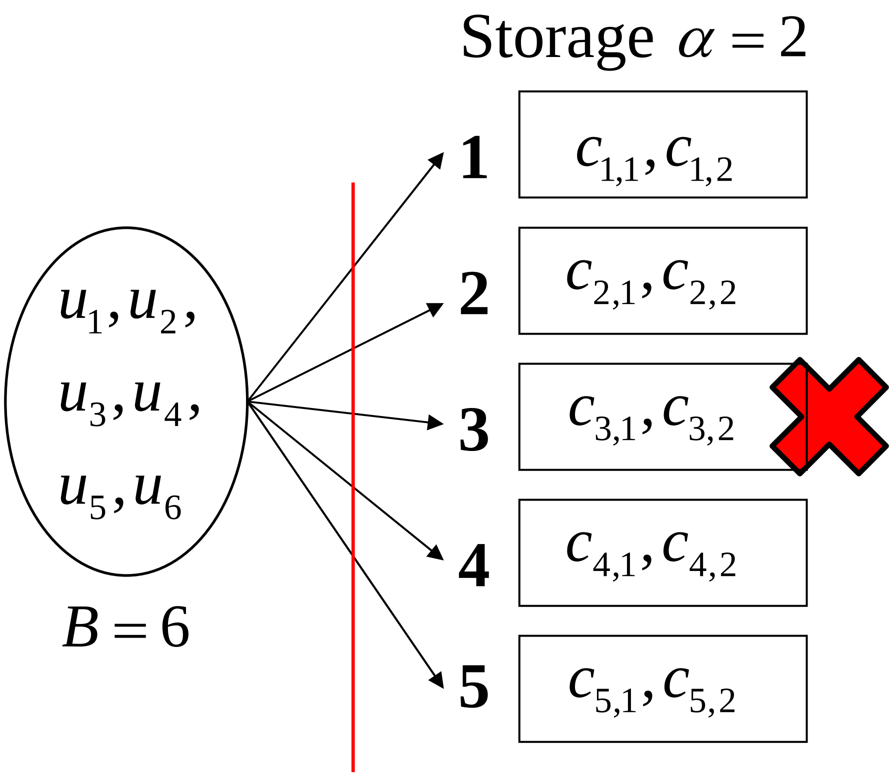
復元（Reconstruction）

$(k=3)$



$$\boxed{H(u_1 u_2 u_3 u_4 u_5 u_6 \mid c_{1,1} c_{1,2} c_{2,1} c_{2,2} c_{4,1} c_{4,2}) = 0}$$

故障ノードの修復問題（Repair Problem） $(k=3)$



「アクセスできない」
と仮定する

故障ノードの修復

1．故障したノードを新しいノードに置き換える。

2．そして、故障ノードが保存していた分散データの複製を保存したい。（再生成）

ただし、再び、ソースから分散データを受信することはできないと仮定する。

修復(再生性)(自明な方法)

$(k,d)=(3,3)$

3個のノードにアクセス

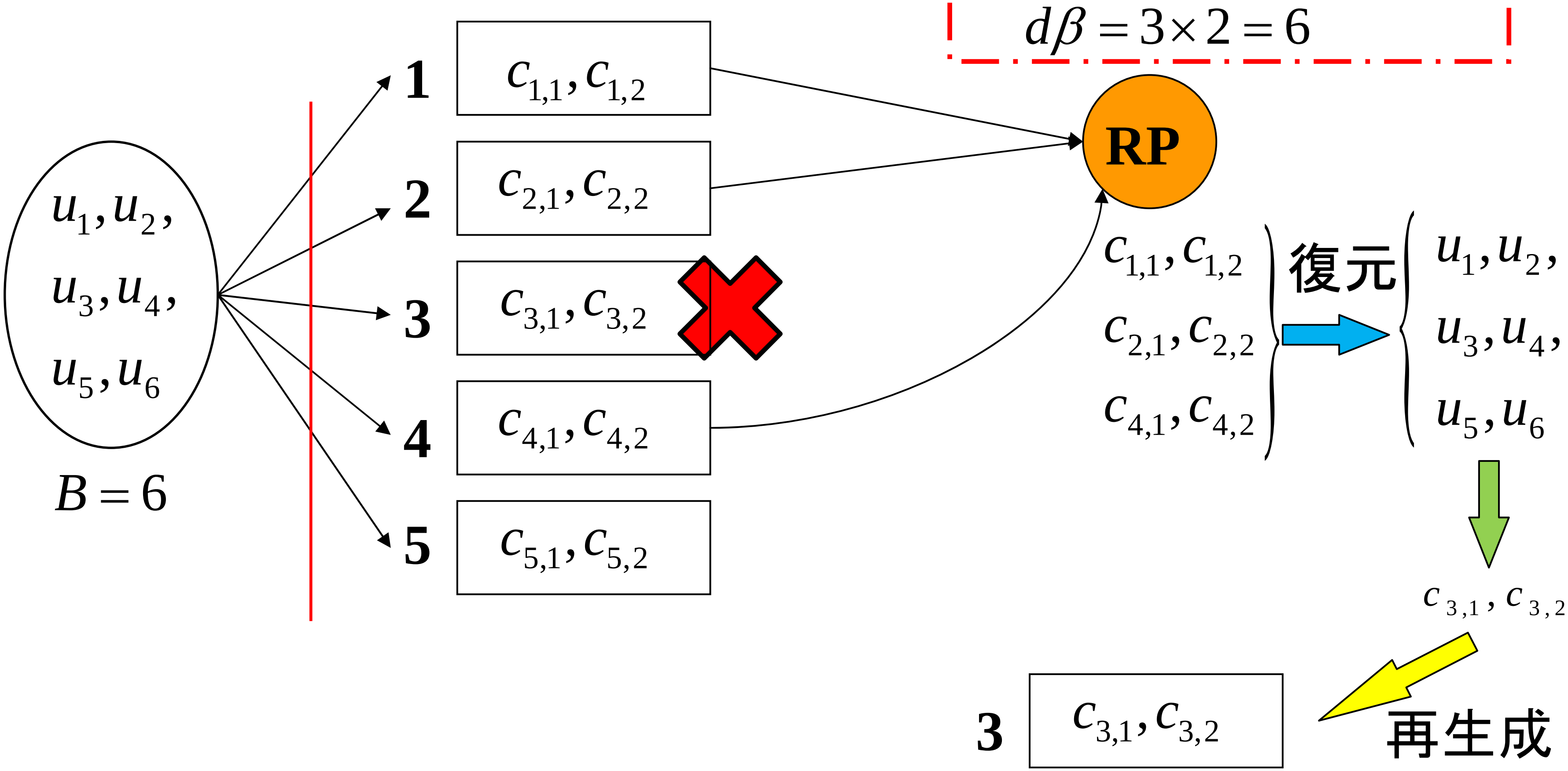
修復バンドワイドト

ストレージ

Storage $\alpha=2$

Repair Bandwidth

$d\beta=3\times2=6$



修復(再生性)：（自明でない方法）

$(k,d)=(3,4)$

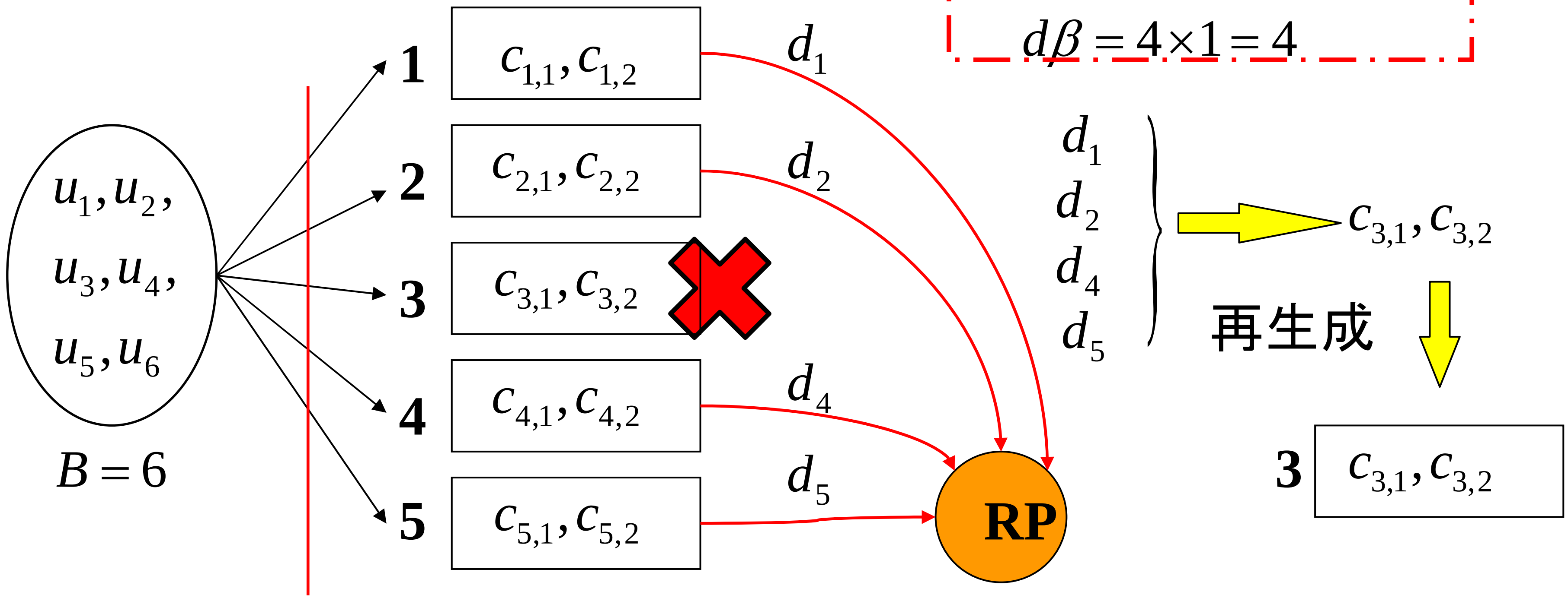
4個のノードにアクセス

修復バンドワイドト

ストレージ　Storage　$\alpha = 2$

Repair Bandwidth

$d\beta = 4 \times 1 = 4$



符号化

$c_{i,1}, c_{i,2}$ → d_i

分散データ　　再生成用データ

$u_k, c_{j,k}, d_l \in GF(q)$

Masazumi Kurihara (Univ. of Electro Communications, Tokyo)

再生成符号 I

1. 「**ストレージ** α」と「**修復バンドワイド** $d\beta$」のトレードオフ関係
   1. 修復バンドワイドを最小:
      → **最小バンドワイド再生成符号**
      (Minimum Bandwidth Regenerating(MBR) codes)
   2. ストレージを最小:
      → **最小ストレージ再生成符号**
      (Minimum Storage Regenerating(MSR) codes)
2. 一般的な再生成符号の一構成方法
   [2] K.V.Rashmi, N.B.Shah, and P.V.Kumar, "Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction," 2010.
   → **Rashmi-Shah-Kumar MSR 符号**

本稿の目的（提案） I

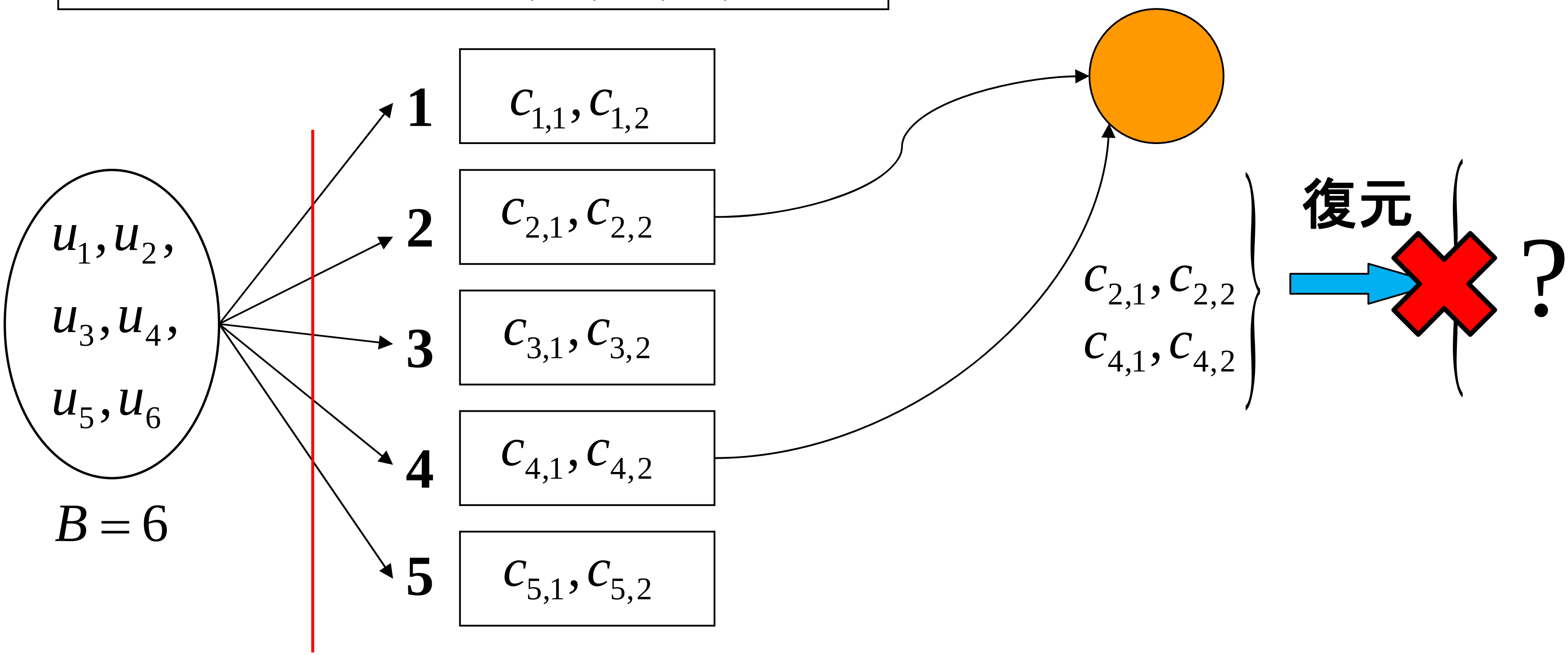
先行研究 : [3] “**分散ストレージにおける再生成符号と秘密分散について**” 2011

（Rashmi-Shah-Kumar MSR **符号を用いた「秘密分散構造の構築方法」と「その安全性」**）

1. Rashmi-Shah-Kumar MSR **符号の拡張 → 「拡張符号」**
   1. **復元方法（ただし、自明な方法と特別な場合の方法）**
   2. **修復方法（再生成の方法）**
2. **安全性（秘密分散）**
   1. **分散データの安全性**
      （ストレージノードが保存するデータ）
   2. **再生成用データの安全性**
      （故障ノードを修復する際に利用するデータ）

「分散データ」の安全性(秘密分散　その1)

$$\boxed{H(u_2u_5)-H(u_2u_5 \mid c_{2,1}c_{2,2}c_{4,1}c_{4,2})=0}$$



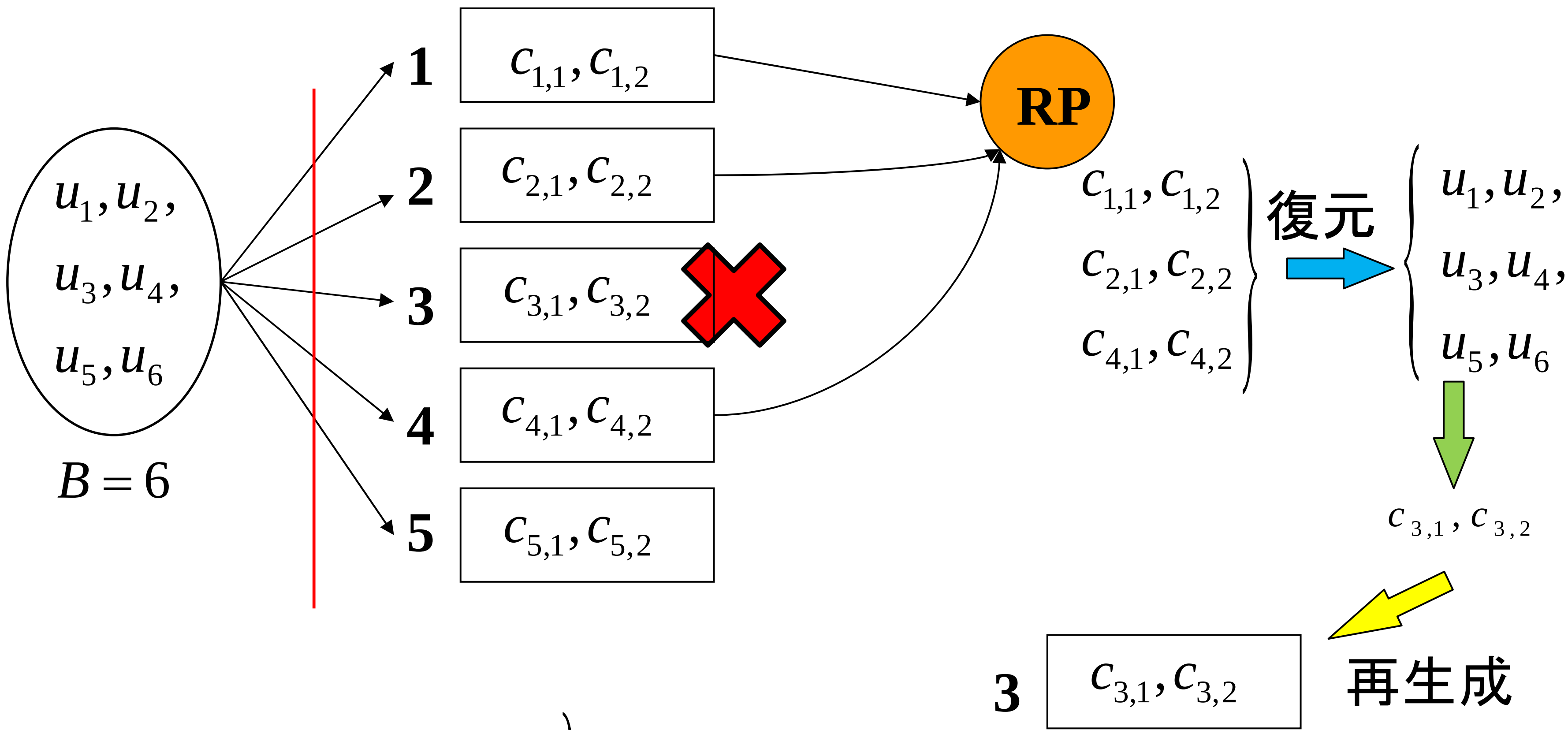
$$\left.\begin{array}{r} \text{秘密情報}: u_2, u_5 \\ \text{乱数}: u_1, u_3, u_4, u_6 \end{array}\right\}$$

Masazumi Kurihara (Univ. of Electro Communications, Tokyo)

修復：　自明な方法における修復と安全性

$$H(u_2u_5) - H(u_2u_5 \mid c_{1,1}c_{1,2}c_{2,1}c_{2,2}c_{4,1}c_{4,2}) = H(u_2u_5)$$

$$(k,d) = (3,3)$$

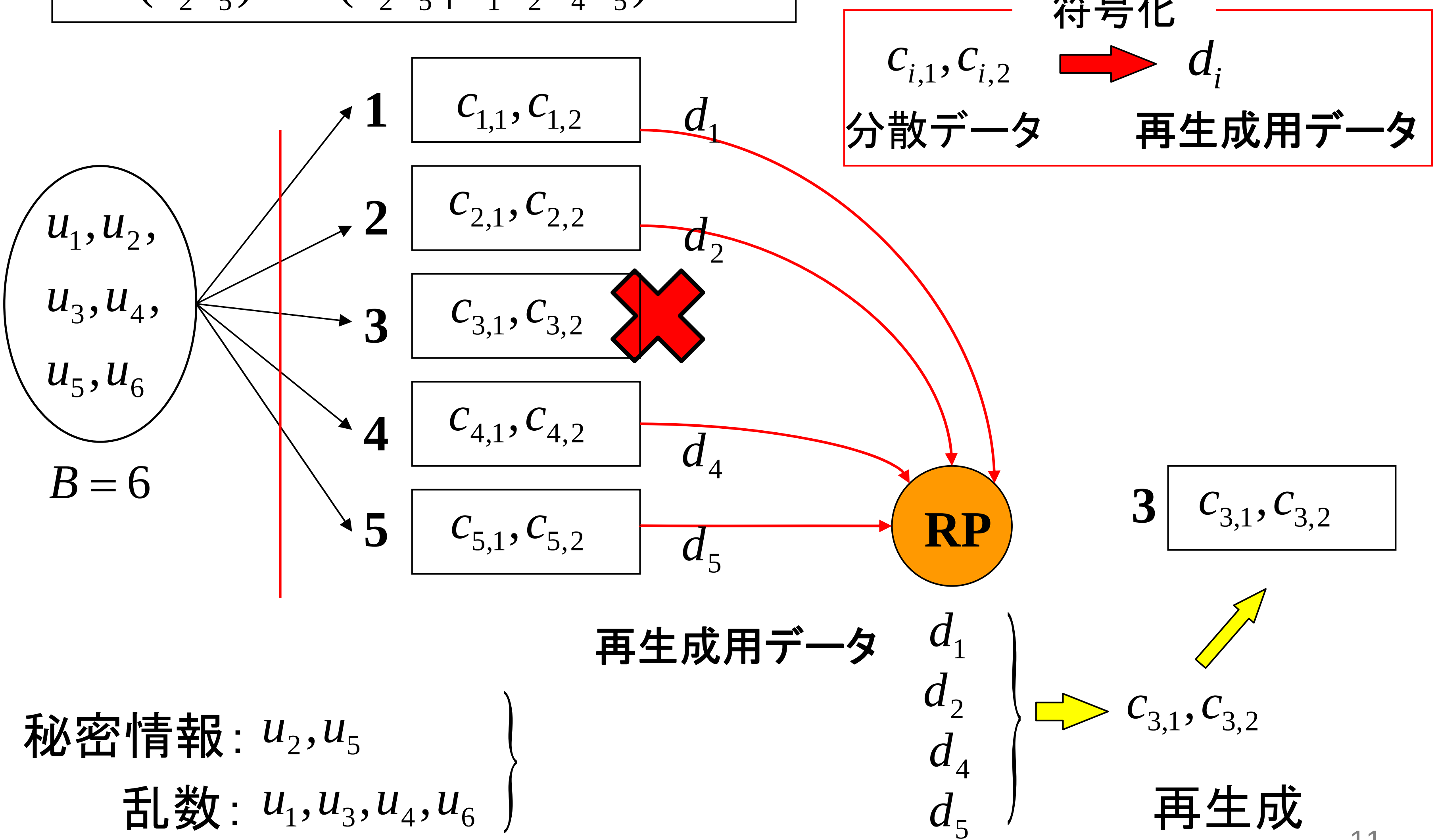


$$\left.\begin{array}{r} \text{秘密情報：} u_2, u_5 \\ \text{乱数：} u_1, u_3, u_4, u_6 \end{array}\right\}$$

Masazumi Kurihara (Univ. of Electro Communications, Tokyo)

修復:「再生成用データ」の安全性(秘密分散　その2)

$$H(u_2u_5) - H(u_2u_5 \mid d_1d_2d_4d_5) = 0$$



秘密情報: u_2, u_5

乱数: u_1, u_3, u_4, u_6

パラメータ（拡張符号） I

1. パラメータ $(n, k, d, \alpha, \beta, B, \delta)$

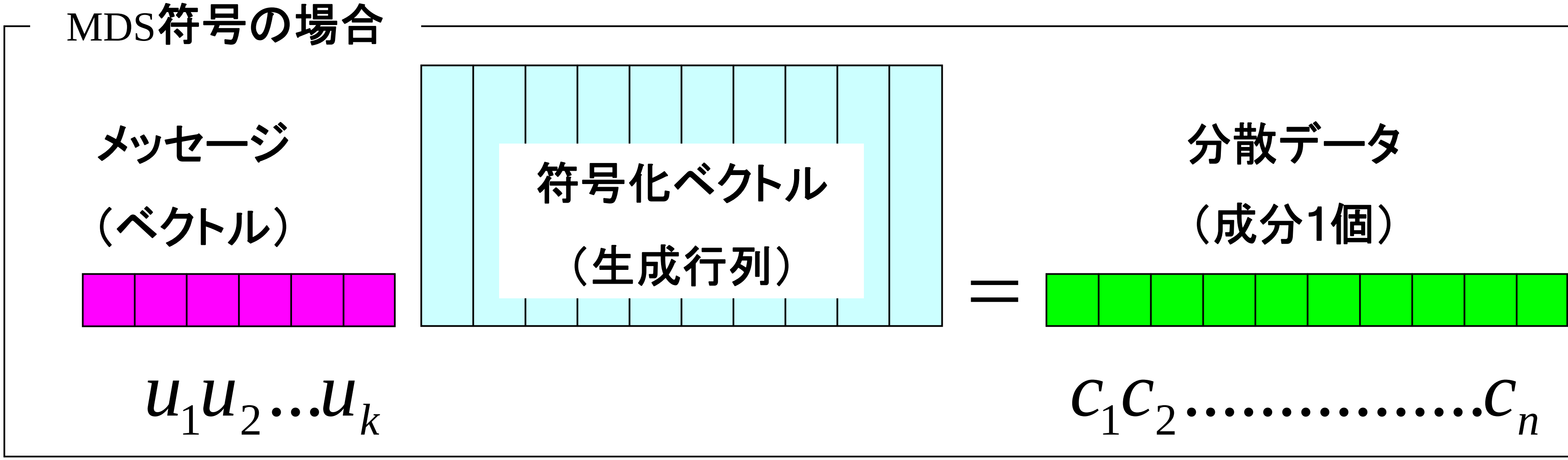
   n ： ストレージノードの個数（分散データの個数）
   k ： 復元のためにアクセスするノードの個数
   d ： 修復のためにアクセスするノードの個数
   α ： 分散データのサイズ
   β ： 再生成データのサイズ ($\beta = 1$)
   B ： メッセージのデータサイズ
   δ ： メッセージ行列中の対称行列の個数 → $1 \leq \delta$
   (オリジナルの Rashmi-Shah-Kumar MSR 符号では $\delta = 2$)

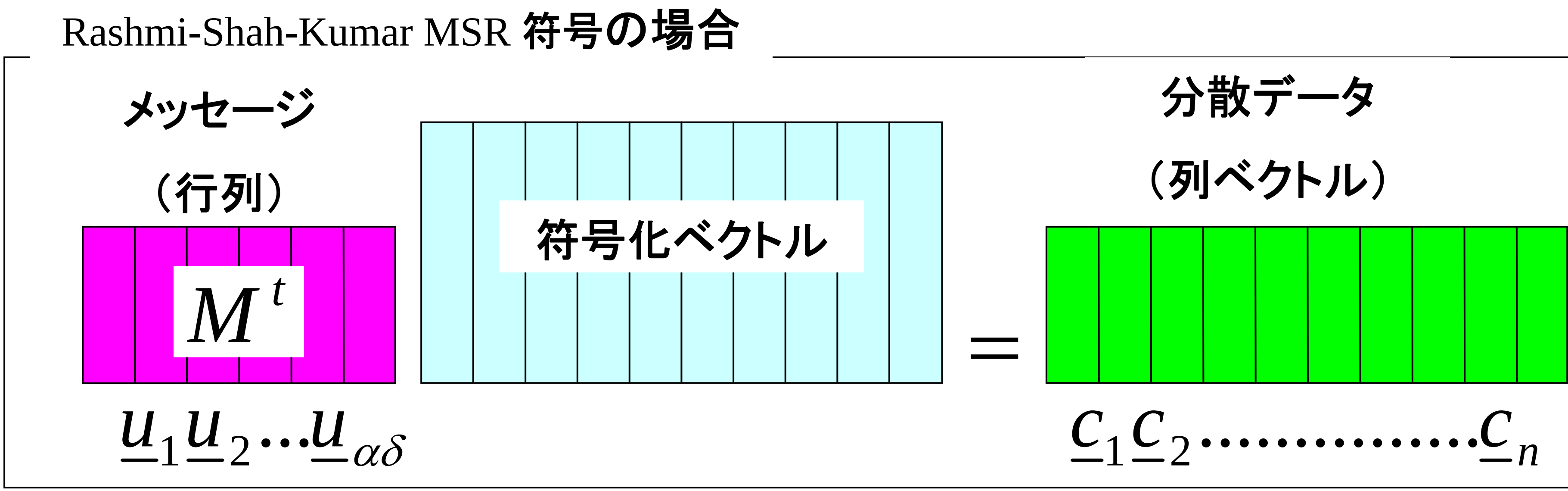
2. パラメータ設定

$$d = \alpha\delta$$

$$B = \frac{\alpha(\alpha + 1)\delta}{2}$$

Rashmi-Shah-Kumar MSR 符号の符号化の様子





メッセージ行列（拡張符号） I

1. $\alpha \times \alpha$ **対称行列**：

$$S^{(l)} = \begin{bmatrix} u_{1,1}^{(l)} & u_{1,2}^{(l)} & \cdots & u_{1,\alpha}^{(l)} \\ u_{2,1}^{(l)} & u_{2,2}^{(l)} & \cdots & u_{2,\alpha}^{(l)} \\ \vdots & \vdots & \ddots & \vdots \\ u_{\alpha,1}^{(l)} & u_{\alpha,2}^{(l)} & \cdots & u_{\alpha,\alpha}^{(l)} \end{bmatrix}, \quad 1 \leq l \leq \delta,$$

2. $\delta\alpha \times \alpha$ **メッセージ行列**：

$$M = \begin{bmatrix} S^{(1)} \\ S^{(2)} \\ \vdots \\ S^{(\delta)} \end{bmatrix}$$

異なる成分の個数 $= \frac{\alpha(\alpha+1)}{2} \times \delta = B$: **メッセージのサイズ**

分散データ（拡張符号） I

1. **分散データ （分散符号化）**
   ノード i の分散データ （サイズは α）：

$$
\begin{aligned}
\underline{c}_i &= \underbrace{\left[c_{i,1}, c_{i,2}, \ldots, c_{i,\alpha}\right]^t}_{\alpha} \\
&= \underbrace{\left[1, x_i, x_i^2, \ldots, x_i^{\alpha\delta-1}\right]}_{\alpha\delta} M \in \mathbb{F}_q^{\alpha\delta}
\end{aligned}
$$

   ただし、ノード $i \in \{1, 2, \ldots, n\}$ に対し、非零な有限体の要素 $x_i \in \mathbb{F}_q$ を対応させ、かつ、$x_i \neq x_j$ if $i \neq j$.

2. **符号化ベクトル**
   ノード i の符号化ベクトル：

$$
\underbrace{\left[1, x_i, x_i^2, \ldots, x_i^{\alpha\delta-1}\right]^t}_{\alpha\delta} \in \mathbb{F}_q^{\alpha\delta}
$$

復元（拡張符号） I

1. 復元（自明な方法）
収集する分散データのサイズ $\alpha^2\delta$

$$\alpha^2\delta \geq \frac{\alpha(\alpha+1)\delta}{2} = B$$

→（効率が良くない）

2. 復元（自明でない方法 $\alpha = 2$）
収集する分散データのサイズ 3δ

$$3\delta = \frac{\alpha(\alpha+1)\delta}{2} = B$$

修復（再生成）（拡張符号）：再生成用データ I

1. 修復（再生成）：故障ノード f の修復
故障していない任意の $d = \alpha\delta$ 個のノード $h_1, h_2, \ldots, h_{\alpha\delta}$ の「分散データ $\underline{c}_{h_p}$」と「故障ノードの符号化ベクトル（の一部）」から得られるサイズ $\beta = 1$ の**再生成用データ**

$$d_{h_p} = \underline{c}_{h_p}^t \underbrace{\left[1, x_f, x_f^2, \ldots, x_f^{\alpha-1}\right]^t}_{\alpha} \in \mathbb{F}_q, \ 1 \le p \le \alpha\delta,$$

をダウンロードする。
このとき、合計サイズ $\alpha\delta$ の再生成データから故障ノードの分散データ $\underline{c}_f$ を再生成できる。すなわち、

$$H(\underline{c}_f | d_{h_1} d_{h_2} \cdots d_{h_{\alpha\delta}}) = 0$$

が成り立つ。

秘密分散の設定 I

文献 [3] にて提案した秘密分散の構築手法を用いる。

1. サイズ B のメッセージの構成を乱数と秘密情報に分ける。
   1. 乱数 $\underline{u}_{\mathrm{r}} \in \mathbb{F}_q^{\alpha\delta}$ ：メッセージ行列内の対称行列の対角成分
      → サイズ $\alpha\delta$
   2. 秘密情報 $\underline{u}_{\mathrm{s}} \in \mathbb{F}_q^{\frac{\alpha(\alpha-1)\delta}{2}}$ ：上記以外の成分:
      → サイズ $\dfrac{\alpha(\alpha-1)\delta}{2}$
2. メッセージ行列

$$M = \begin{bmatrix} S^{(1)} \\ S^{(2)} \\ \vdots \\ S^{(\delta)} \end{bmatrix} \quad \text{where} \quad S^{(l)} = \begin{bmatrix} u_{1,1}^{(l)} & u_{1,2}^{(l)} & \cdots & u_{1,\alpha}^{(l)} \\ u_{2,1}^{(l)} & u_{2,2}^{(l)} & \cdots & u_{2,\alpha}^{(l)} \\ \vdots & \vdots & \ddots & \vdots \\ u_{\alpha,1}^{(l)} & u_{\alpha,2}^{(l)} & \cdots & u_{\alpha,\alpha}^{(l)} \end{bmatrix}$$

分散データの安全性（秘密分散 その１） I

定理 任意の δ 個のノード $i_1, i_2, \ldots, i_\delta$ が保存する合計サイズ $\alpha\delta$ の分散データ

$$\underbrace{\underline{c}_{i_1}, \underline{c}_{i_2}, \ldots, \underline{c}_{i_\delta}}_{\delta}$$

から秘密情報 $\underline{u}_{\mathrm{S}}$ はまったくもれない。すなわち、

$$H(\underline{u}_{\mathrm{S}}^t) - H(\underline{u}_{\mathrm{S}}^t | \underline{c}_{i_1}^t \underline{c}_{i_2}^t \cdots \underline{c}_{i_\delta}^t) = 0$$

が成り立つ。

分散データの安全性（秘密分散 その１）：説明 I

1. 「分散データ」と「乱数と秘密情報」の関係式：

$$\begin{bmatrix} c_{i_1,1} \\ c_{i_2,1} \\ \vdots \\ c_{i_\delta,\alpha} \end{bmatrix} = \begin{bmatrix} \underset{(\alpha\delta \times \alpha\delta)}{C_{\alpha\delta}} & \underset{(\alpha\delta \times (\alpha(\alpha-1)\delta/2)}{\overline{C}_{\alpha\delta}} \end{bmatrix} \begin{bmatrix} \underline{u}_{\mathrm{r}} \\ \underline{u}_{\mathrm{s}} \end{bmatrix}$$

2. サイズ $\alpha\delta$ の乱数 $\underline{u}_{\mathrm{r}}$ に対応する $\alpha\delta \times \alpha\delta$ 行列 $C_{\alpha\delta}$ の行列式は、

$$\det C_{\alpha\delta} \neq 0$$

となる。ただし、次の条件を満たす必要がある：

条件：任意の異なる要素 $x_i, x_j \in \{x_1, x_2, \ldots, x_n\}$ に対し、$x_i^\alpha \neq x_j^\alpha$ が成り立つ。

再生成用データの安全性（秘密分散 その２） I

定理 故障していない任意の $d = \alpha\delta$ 個のノード $h_1, h_2, \ldots, h_{\alpha\delta}$ からダウンロードした合計サイズ $\alpha\delta$ の再生成用データ

$$\underbrace{d_{h_1}, d_{h_2}, \ldots, d_{h_{\alpha\delta}}}_{\alpha\delta}$$

からから秘密情報 $\underline{u}_{\mathrm{S}}$ はまったくもれない。すなわち、

$$H(\underline{u}_{\mathrm{S}}^t) - H(\underline{u}_{\mathrm{S}}^t | d_{h_1} d_{h_2} \cdots d_{h_{\alpha\delta}}) = 0$$

が成り立つ。

再生成用データの安全性（秘密分散 その２）：説明 I

1. 「再生成用データ」と「乱数と秘密情報」の関係式：

$$\begin{bmatrix} d_{h_1} \\ d_{h_2} \\ \vdots \\ d_{h_{\alpha\delta}} \end{bmatrix} = \begin{bmatrix} \underset{(\alpha\delta\times\alpha\delta)}{D_{\alpha\delta}} & \underset{(\alpha\delta\times(\alpha(\alpha-1)\delta/2)}{\overline{D}_{\alpha\delta}} \end{bmatrix} \begin{bmatrix} \underline{u}_{\mathrm{r}} \\ \underline{u}_{\mathrm{s}} \end{bmatrix}$$

2. サイズ $\alpha\delta$ の乱数 $\underline{u}_{\mathrm{r}}$ に対応する $\alpha\delta\times\alpha\delta$ 行列 $D_{\alpha\delta}$ の行列式は，

$$\det D_{\alpha\delta} \neq 0$$

となる。

結論

本稿では、分散ストレージシステムの修復問題において、以下のことを示した:

1. Rashmi-Shah-Kumar MSR 符号の拡張 → 「拡張符号」
   1. 再生成符号（復元と再生成）
2. 安全性（秘密分散）
   1. 分散データの安全性
      任意の δ 個のノードが保存するサイズ $\alpha\delta$ の
      分散データに対する秘密分散の安全性
   2. 再生成用データの安全性
      故障ノードを修復するためのサイズ $\alpha\delta$ の
      任意の再生成用データに対する秘密分散の安全性

参考文献

1. [1] A.G.Dimakis, P.B.Godfrey, Y.Wu, M.J.Wainwright and K.Ramchandran,

   ”Network Coding for Distributed Storage Systems,”

   IEEE Trans. on Information Theory, vol.56, no.9, pp.4539–4551, Sept. 2010.

2. [2] K.V.Rashmi, N.B.Shah, and P.V.Kumar,

   “Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction,”

   http://arxiv.org/abs/1005.4178

3. [3] **栗原正純**, **桑門秀典**,

   “**分散ストレージにおける再生成符号と秘密分散について**,”

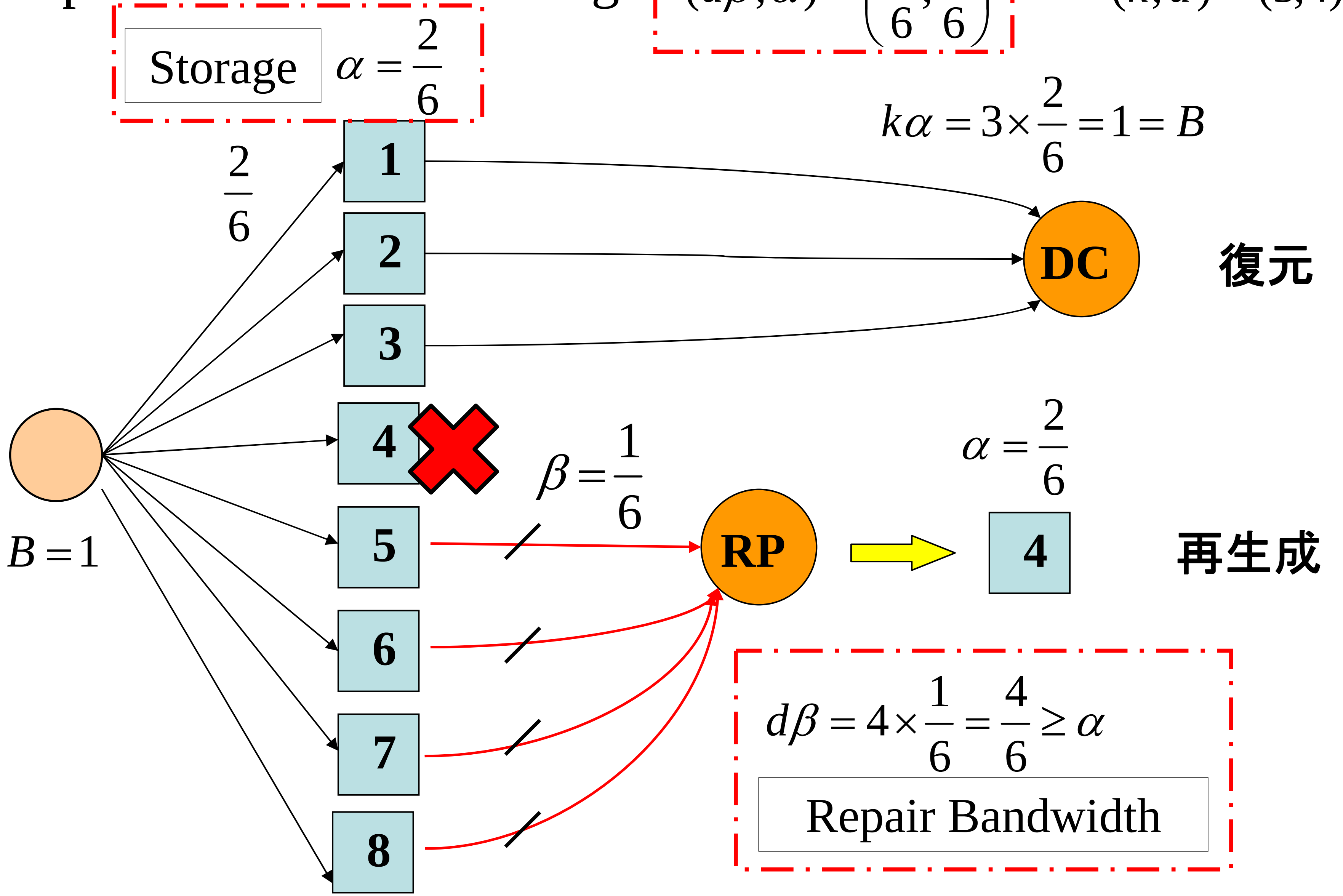
   信学技法, IT2010-56(2011-01), pp.13-18, Jan, 2011.

追加資料(additional slides)

再生成符号 I

1. 「**ストレージ** α」と「**修復バンドワイド** $d\beta$」のトレードオフ関係
   1. 修復バンドワイドを最小:
      → **最小バンドワイド再生成符号**
      (Minimum Bandwidth Regenerating(MBR) codes)
   2. ストレージを最小:
      → **最小ストレージ再生成符号**
      (Minimum Storage Regenerating(MSR) codes)
2. 一般的な再生成符号の一構成方法
   [2] K.V.Rashmi, N.B.Shah, and P.V.Kumar,
   "Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction," 2010.
   → Rashmi-Shah-Kumar MSR 符号

Repair Bandwidth – Storage $(d\beta, \alpha) = \left(\frac{4}{6}, \frac{2}{6}\right)$ for $(k, d) = (3,4)$

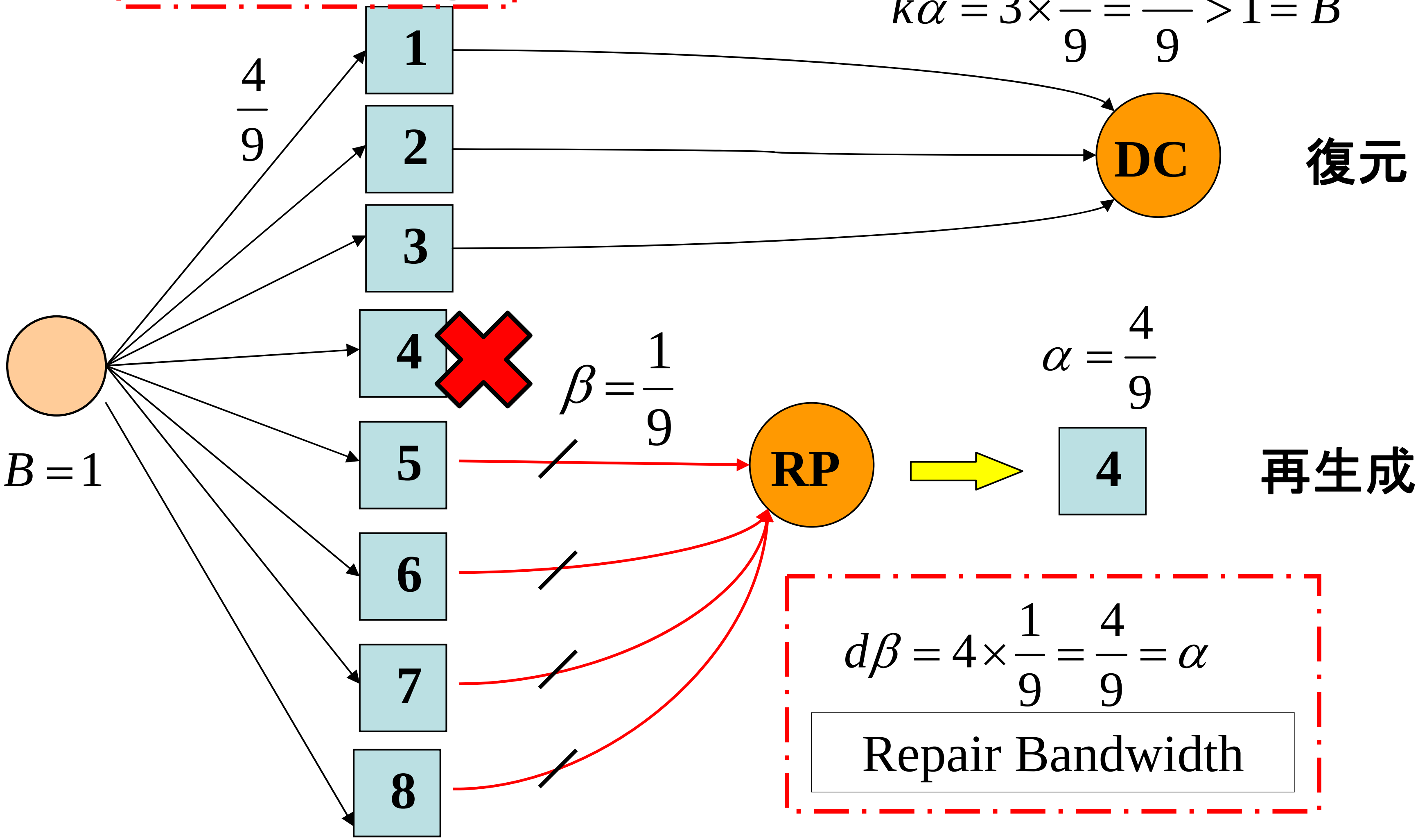


Repair Bandwidth - Storage

$$(d\beta, \alpha) = \left(\frac{4}{9}, \frac{4}{9}\right) \text{ for } (k, d) = (3,4)$$

Storage $\alpha = \frac{4}{9}$

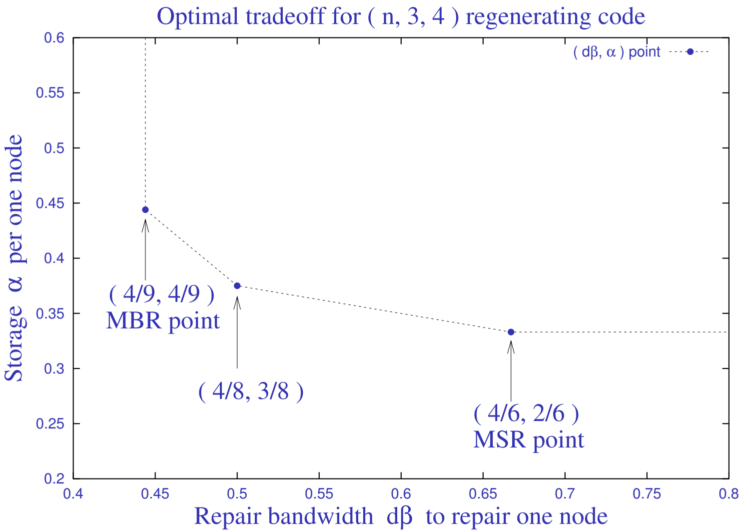
$$k\alpha = 3 \times \frac{4}{9} = \frac{12}{9} > 1 = B$$



$$d\beta = 4 \times \frac{1}{9} = \frac{4}{9} = \alpha$$

Repair Bandwidth

Tradeoff curve between strage α and repair bandwidth $d\beta$ I



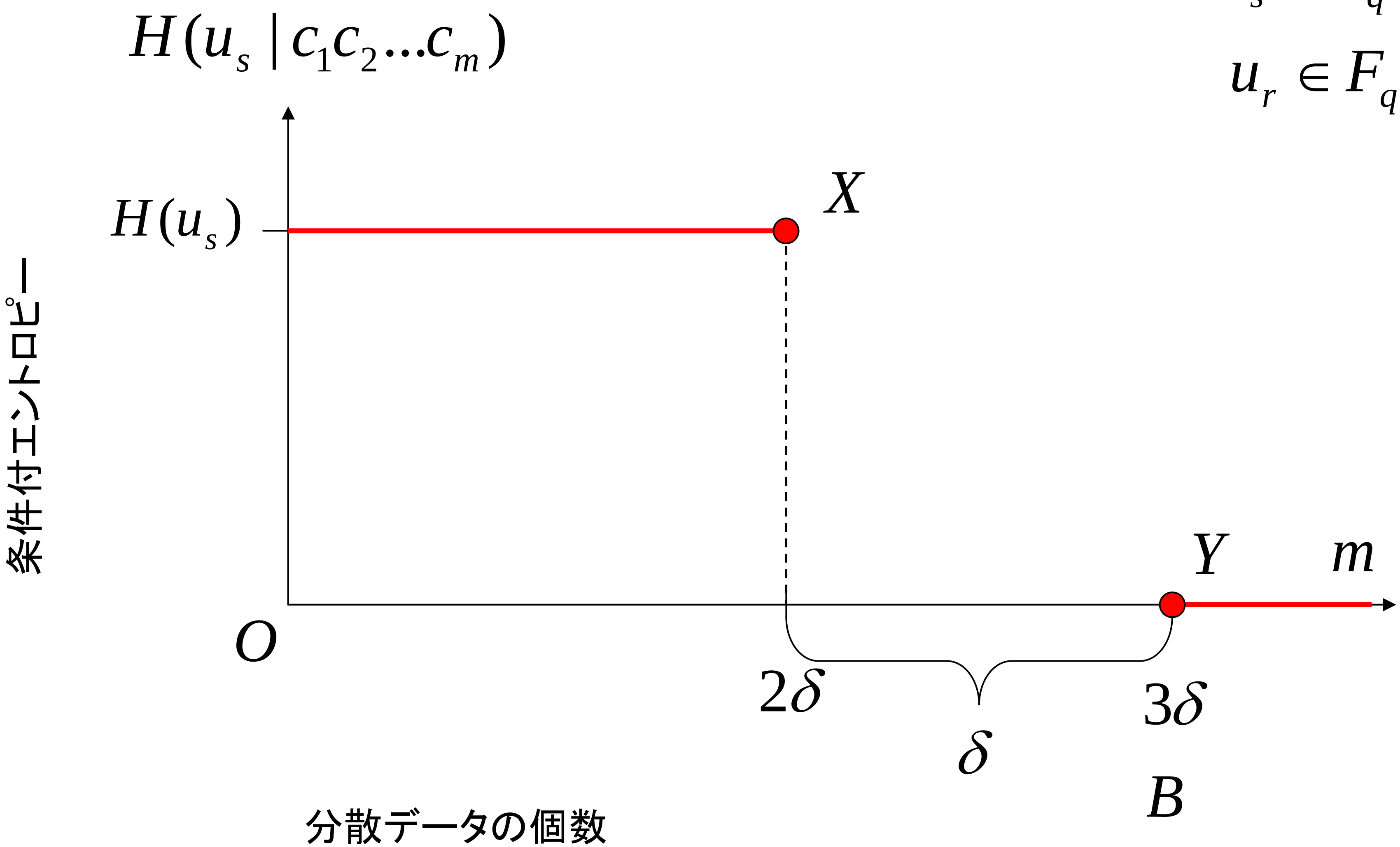
Optimal tradeoff curve between strage α and repair bandwidth $d\beta$ for $(k, d) = (3, 4)$ and $B = 1$.

ランプ型: $H(u_s \mid c_1 c_2 \ldots c_m)$

$\alpha = 2$

$u_s \in F_q^{\ \delta}$

$u_r \in F_q^{\ 2\delta}$



Masazumi Kurihara (Univ. of Electro Communications, Tokyo)

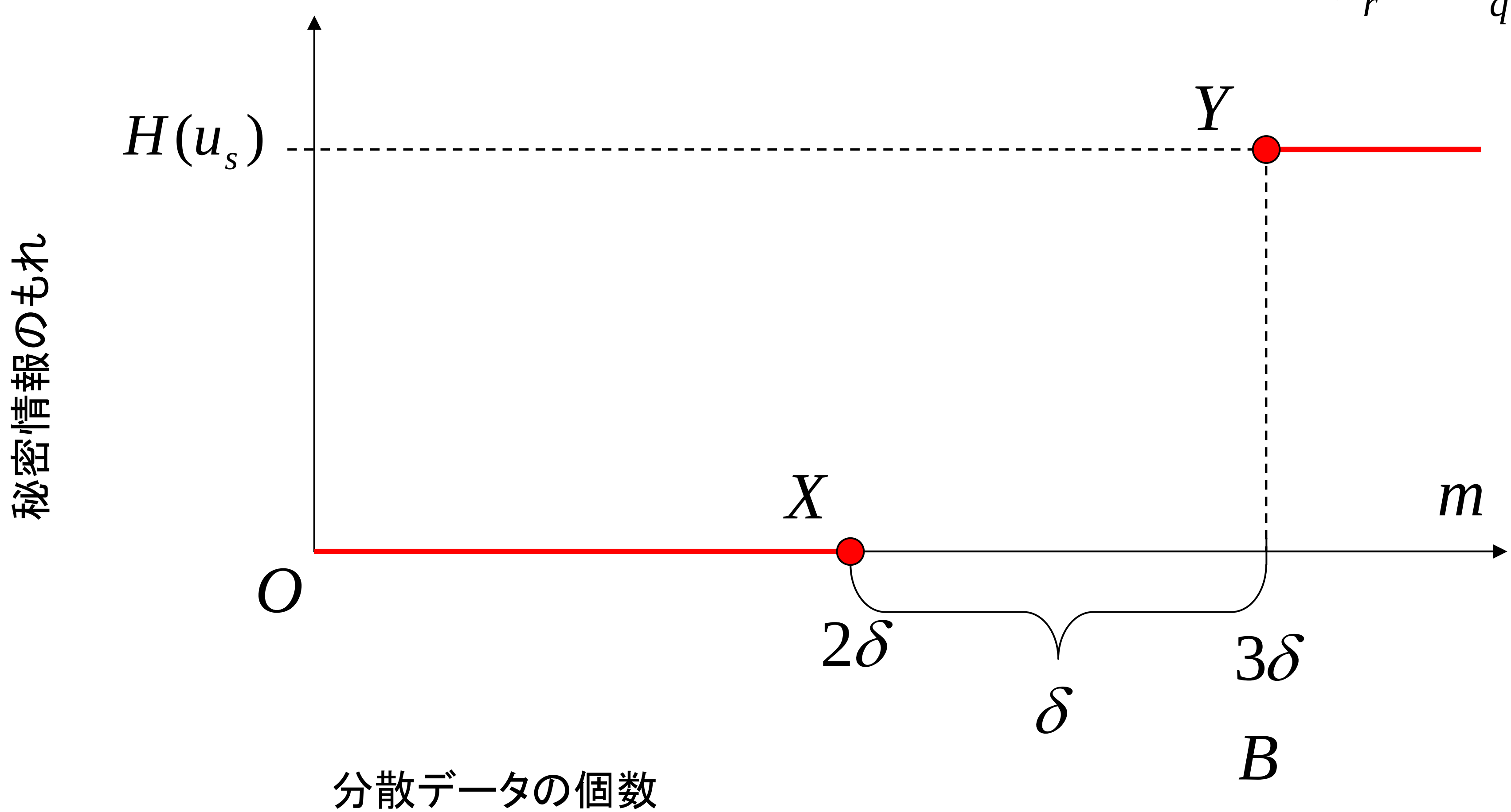
ランプ型: $H(u_s)-H(u_s\,|\,c_1c_2\ldots c_m)$

$$\alpha = 2$$

$$u_s \in F_q^{\ \delta}$$

$$u_r \in F_q^{\ 2\delta}$$

$H(u_s)-H(u_s\,|\,c_1c_2\ldots c_m)$



Masazumi Kurihara (Univ. of Electro Communications, Tokyo)